Instalación y configuración de VMware Horizon Mobile Manager

Horizon Mobile Manager 1.2

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte http://www.vmware.com/support/pubs.

ES-000994-00

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

http://www.vmware.com/es/support/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Guía de instalación y configuración de VMware Horizon Mobile Manager

Guía de instalación y configuración de VMware Horizon Mobile Manager proporciona información acerca de cómo instalar y configurar la aplicación virtual Horizon Mobile Manager de VMware.

La aplicación virtual Horizon Mobile Manager proporciona los componentes del lado del servidor que se utilizan en la solución Horizon Mobile. El proceso de instalación y configuración general de los componentes del lado del servidor implica:

1 Determinar qué configuración de implementación se va a utilizar

2 Implementar la aplicación virtual

3 Poner en marcha la aplicación virtual

4 Configurar ajustes para la propia aplicación

5 Instalar y configurar los elementos necesarios para la configuración de implementación elegida

6 Configurar los ajustes de Horizon Mobile Manager, según la configuración de implementación elegida

7 Reiniciar para aplicar los ajustes seleccionados

8 Determinar el método de certificación de identidad digital adecuado y, opcionalmente, sustituir los certificados predeterminados

Destinatarios

Esta información está destinada a los administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Configuraciones de implementación 1

Horizon Mobile Manager está diseñado para controlar, personalizar y gestionar áreas de trabajo corporativas en los dispositivos móviles de los usuarios. La configuración de implementación de Horizon Mobile Manager de su empresa debe permitir la gestión del área de trabajo en el dispositivo sin ninguna limitación, independientemente de si el dispositivo se comunica con Horizon Mobile Manager a través de la red corporativa o por Internet.

La aplicación virtual Horizon Mobile Manager incluye un servidor Apache 2.2 que proporciona capacidades de gestión del lado del servidor. En la tabla siguiente se describen las configuraciones de implementación típicas de Horizon Mobile Manager.

Tabla 1-1. Configuraciones de implementación de Horizon Mobile Manager

Configuración	Descripción	Pros	Contras
Horizon Mobile Manager en zonas desmilitarizadas de Internet (DMZ).	En la entornos de redes, una DMZ de Internet es una zona de confianza combinada entre los servicios de red internos e Internet. En esta configuración, la dirección IP de Horizon Mobile Manager es una dirección IP pública externa y se puede acceder a ella directamente por Internet. Los dispositivos se comunican con solicitudes SSL a la dirección IP pública de Horizon Mobile Manager.	■ La forma más sencilla de poner en marcha Horizon Mobile Manager. ■ No se necesita ninguna configuración de red especial, aparte de una dirección IP externa.	■ No es apropiada para entornos de producción, porque todos los servicios de Horizon Mobile Manager se exponen públicamente en Internet. ■ No se puede configurar Horizon Mobile Manager para conectarse a servicios internos de empresa como Active Directory, LDAP o servicios de bases de datos corporativas sin abrir puertos a través del firewall de la empresa.
Con Horizon Mobile Manager en la red interna de la empresa y traduciendo la dirección IP de Horizon Mobile Manager a una dirección IP disponible en el exterior mediante la traducción de direcciones de red (NAT).	En esta configuración, Horizon Mobile Manager tiene una dirección IP privada. Los dispositivos se comunican mediante solicitudes SSL a una dirección IP disponible en el exterior. Dichas solicitudes SSL deben traducirse a la dirección IP privada de Horizon Mobile Manager con NAT.	■ Los servicios de Horizon Mobile Manager están protegidos por el firewall de la empresa. ■ Horizon Mobile Manager puede conectarse a servicios internos como Active Directory, LDAP o servicios de bases de datos corporativas sin abrir puertos a través del firewall. ■ NAT es una configuración de red conocida y habitual en las empresas.	■ Requiere la definición de reglas de NAT que traduzcan las solicitudes IP al puerto TCP/IP 443 en la dirección IP privada de Horizon Mobile Manager. ■ El puerto 433 de Horizon Mobile Manager debe ser de acceso público. ■ Una arquitectura no del todo satisfactoria para entornos con clústeres de servidores de Horizon Mobile Manager que tengan uno o más servidores Apache de proxy inverso externos.
Con Horizon Mobile Manager en la red interna de la empresa y gestionando las solicitudes SSL de los dispositivos en Internet mediante un servidor de proxy inverso en las DMZ.	En esta configuración, el servidor de proxy inverso finaliza las solicitudes SSL de los dispositivos y, a continuación, inicia nuevas solicitudes para Horizon Mobile Manager en el lado accesible internamente de la red principal. El servidor de proxy inverso convierte las solicitudes de servicios de concesión, descarga e inicio de sesión de Horizon Mobile Manager en URL específicas compatibles con Horizon Mobile Manager.	■ Los servicios de Horizon Mobile Manager están protegidos por el firewall de la empresa. ■ Horizon Mobile Manager puede conectarse a servicios internos como Active Directory, LDAP o servicios de bases de datos corporativas sin abrir puertos a través del firewall. ■ Hay muchas empresas que utilizan de forma asidua servidores de proxy inverso para aislar los servidores de aplicaciones internos de Internet, y estos servidores de proxy	■ Requiere una planificación cuidadosa para configurar el servidor de proxy inverso y las reglas para su comunicación con Horizon Mobile Manager. ■ Requiere la participación de equipos de redes para asegurarse de que el servidor de proxy inverso dispone de una ruta a Horizon Mobile Manager en una interfaz secundaria.

Tabla 1-1. Configuraciones de implementación de Horizon Mobile Manager (Continua)

Configuración	Descripción	Pros	Contras
		pueden ampliarse para que funcionen con Horizon Mobile Manager. ■ Esta configuración es la arquitectura más escalable y segura para la implementación de Horizon Mobile Manager en entornos de producción.	

De las tres configuraciones, la instalación de Horizon Mobile Manager en la DMZ es la forma más rápida de empezar a ver cómo funciona la solución Horizon Mobile. Sin embargo, como esa configuración expone públicamente a Internet los servicios de Horizon Mobile Manager, es la menos segura. El uso de la configuración de DMZ solo (please review updated orthography) debe utilizarse para demostraciones de prueba de concepto y procesos de prueba. En la configuración de DMZ tenga en cuenta la visibilidad de Horizon Mobile Manager y no lo conecte a ningún Active Directory o servidor de base de datos que se esté ejecutando en la red interna. Para las demostraciones de prueba de concepto, utilice los servidores de bases de datos y LDAP integrados instalados con la aplicación virtual Horizon Mobile Manager y asigne usuarios de prueba de ese LDAP integrado a dispositivos móviles concretos para demostrar las capacidades de administración de Horizon Mobile Manager.

Aunque el uso de un servidor proxy inverso implica la configuración más compleja, también es la más segura, y una de las mejores para la implementación de producción.

Instalación de la Aplicación virtual Horizon Mobile Manager 2

Horizon Mobile Manager se distribuye como una aplicación virtual. El primer paso en el proceso de instalación es implementar la aplicación virtual Horizon Mobile Manager.

Es posible instalar la aplicación virtual Horizon Mobile Manager en cualquier plataforma de virtualización compatible con OVF 1.0. Los pasos del proceso describen la implementación en vSphere.

Para implementar la aplicación virtual en vSphere, necesitará un escritorio de Microsoft Windows con vSphere Client instalado.

Prerequisitos

Descargue el archivo OVA de Horizon Mobile Manager de la página de descargas de productos.

Procedimiento

1 Inicie sesión en vSphere Client.

2 Seleccione **Archivo > Implementar plantilla OVF**.

3 Haga clic en **Examinar** y a continuación busque y seleccione la ubicación del archivo OVA de Horizon Mobile Manager.

4 Haga clic en **Siguiente**.

5 Revise los detalles de la plantilla de Horizon Mobile Manager y haga clic en **Siguiente**.

6 Lea y acepte el Contrato de licencia para el usuario final y haga clic en **Siguiente**.

7 Escriba un nombre representativo para la aplicación virtual Horizon Mobile Manager y haga clic en **Siguiente**.

8 Seleccione **Formato de aprovisionamiento fino** y haga clic en **Siguiente**.

9 Revise las opciones que ha elegido y haga clic en **Finalizar**.

   Un mensaje de progreso indica que la aplicación virtual Horizon Mobile Manager se está implementando y un mensaje de éxito indica cuándo ha finalizado la implementación.

Qué hacer a continuación

Active y configure la aplicación virtual Horizon Mobile Manager. Consulte Capítulo 3, “Configuración de la Aplicación virtual Horizon Mobile Manager,” página 13.

Configuración de la Aplicación virtual Horizon Mobile Manager 3

Configure el adaptador de red para la aplicación virtual y enciéndala. Tras encender la aplicación virtual, configure la propia aplicación cambiando la contraseña predeterminada, configurando una dirección IP estática y configurando los ajustes de red de la aplicación.

Prerequisitos

Instale la aplicación virtual Horizon Mobile Manager. Consulte Capítulo 2, "Instalación de la Aplicación virtual Horizon Mobile Manager," página 11.

Determine qué configuración de implementación se va a utilizar. Consulte Capítulo 1, "Configuraciones de implementación," página 7.

Procedimiento

1 En vSphere Client, en la pestaña **Introducción** de la aplicación virtual, haga clic en **Editar configuración de máquina virtual**.

2 En la pestaña **Hardware**, configure el adaptador de red para la aplicación virtual, según las opciones apropiadas para la implementación elegida.

Configuración de implementación	Descripción
Horizon Mobile Manager en su DMZ	Conéctese a una interfaz de red en su DMZ.
Horizon Mobile Manager en su red interna, utilizando NAT para traducir una IP pública a la IP interna	Conéctese a una interfaz de red en su red interna.
Horizon Mobile Manager en su red interna, utilizando un servidor proxy inverso para delegar solicitudes externas a la IP interna	Conéctese a una interfaz de red en su red interna.

3 Active la aplicación virtual Horizon Mobile Manager en vSphere Client y haga clic en la pestaña **Consola**.

La aplicación virtual muestra mensajes mientras se está encendiendo. Lea y acepte el Contrato de licencia para el usuario final.

4 Cuando se active la aplicación virtual y aparezca el menú principal, seleccione **Iniciar sesión**.

5 Inicie sesión en el sistema operativo Linux de la aplicación virtual utilizando los valores predeterminados de la aplicación: nombre de usuario **`root`** y contraseña **`vmware`**.

6 Por motivos de seguridad, cambie la contraseña predeterminada "root".

7 Escriba **`exit`** para volver al menú principal.

8 Seleccione **Configurar red**.

9 Configure los ajustes de red para adecuarlos a la configuración de implementación que haya elegido.

Configuración de implementación	Descripción
Horizon Mobile Manager en su DMZ	Configure los ajustes de red de la aplicación para utilizar una dirección IP estática. Siga las indicaciones para configurar la dirección IP, la máscara de red, la puerta de enlace, los servidores DNS y el nombre de host.
Horizon Mobile Manager en su red interna, utilizando NAT para traducir una IP pública a la IP interna	a Configure los ajustes de red de la aplicación para utilizar una dirección IP estática interna. Siga las indicaciones para configurar la dirección IP, la máscara de red, la puerta de enlace, los servidores DNS y el nombre de host. Si la red interna requiere el uso de un servidor proxy de reenvío, configure el servidor proxy. b Cree reglas de NAT en su firewall para asignar el puerto TCP/IP 443 a la dirección IP interna de la aplicación.
Horizon Mobile Manager en su red interna, utilizando un servidor proxy inverso para delegar solicitudes externas a la IP interna	a Configure los ajustes de red de la aplicación para utilizar una dirección IP estática. Siga las indicaciones para configurar la dirección IP, la máscara de red, la puerta de enlace, los servidores DNS y el nombre de host. Si la red interna requiere el uso de un servidor proxy de reenvío, configure el servidor proxy. b Configure el servidor proxy inverso con dos interfaces de red: ■ Una interfaz en su DMZ ■ Una interfaz en su red interna c Configure el servidor proxy inverso para habilitar las conexiones HTTPS y cifre el tráfico entre Internet y el servidor proxy mediante conexiones con protocolo Secure Sockets Layer (SSL). d Configure las reglas de proxy para que se soliciten conexiones SSL y para que se deleguen las URL a Horizon Mobile Manager en la red interna: ■ `https://<su_nombre_de_dominio>/provision` ■ `https://<su_nombre_de_dominio>/leasing` ■ `https://<su_nombre_de_dominio>/download` El servidor Apache integrado de Horizon Mobile Manager está configurado para escuchar puertos TCP/IP específicos para determinados tipos de solicitudes. Por lo tanto, si el servidor proxy inverso utiliza los módulos `mod_jk` o `mod_proxy_ajp`, utilice el puerto TCP/IP 8009 para ponerse en contacto con Horizon Mobile Manager. Si el servidor proxy inverso utiliza el módulo `mod_proxy_http`, utilice el puerto TCP/IP 8080 para ponerse en contacto con Horizon Mobile Manager.

Cuando termine de configurar los ajustes de red de la aplicación virtual en la pestaña **Consola**, volverá al menú principal.

La configuración de la aplicación virtual Horizon Mobile Manager habrá finalizado.

Qué hacer a continuación

Conéctese a la interfaz de configuración de Horizon Mobile Manager para añadir claves de licencia y configurar ajustes. Consulte Capítulo 4, “Adición de claves de licencia,” página 15 y Capítulo 5, “Configuración de los ajustes de Horizon Mobile Manager,” página 17.

Adición de claves de licencia 4

Utilice la interfaz de configuración para añadir claves de licencia que habiliten la funcionalidad de gestionar teléfonos profesionales mediante Horizon Mobile Manager. Cada clave de licencia permite que una licencia gestione un número específico de teléfonos profesionales con Horizon Mobile Manager.

Prerequisitos

- Obtenga una o más claves de licencia válidas. También se hace referencia a una clave de licencia como un número de serie en la interfaz de configuración.
- Verifique que está utilizando una versión reciente de los navegadores Chrome, Firefox, Internet Explorer o Safari.

Procedimiento

1 En el navegador, introduzca la URL de la interfaz de configuración de Horizon Mobile Manager, con el formato **`https://`*`dirección_ip`*`:5480`**, donde *dirección_ip* es la que se ha establecido al configurar la propia aplicación virtual.

   La interfaz web utiliza un certificado autofirmado.

2 Inicie sesión como usuario **`root`**.

   Utilice la contraseña que estableció cuando configuró la aplicación virtual Horizon Mobile Manager. Si no ha cambiado la contraseña predeterminada, introduzca **`vmware`** como contraseña.

3 Haga clic en la pestaña **Horizon** y haga clic en **Licencias**.

4 Haga clic en **Agregar licencia de teléfono profesional**.

5 Introduzca la clave de licencia (número de serie) y haga clic en **Agregar**.

Tras introducir una clave de licencia válida, el sistema muestra la información relacionada con la licencia, como la fecha de caducidad de la licencia y el número de teléfonos profesionales que puede gestionar.

Qué hacer a continuación

Si aún no lo ha hecho, configure los ajustes de Horizon Mobile Manager. Debe hacer clic en **Guardar y reiniciar** en la pestaña **Configuración** al menos una vez para finalizar el proceso de instalación de Horizon Mobile Manager. Consulte Capítulo 5, “Configuración de los ajustes de Horizon Mobile Manager,” página 17.

Configuración de los ajustes de Horizon Mobile Manager 5

Debe personalizar determinados ajustes, o aceptar los valores predeterminados, antes de que Horizon Mobile Manager esté listo para utilizarse por primera vez. Debe hace clic en **Guardar y reiniciar** en la pestaña **Configuración** para inicializar los elementos necesarios para configurar las áreas de trabajo del usuario en Horizon Mobile Manager, como la imagen base del área de trabajo.

Prerequisitos

- Verifique que está utilizando una versión reciente de los navegadores Chrome, Firefox, Internet Explorer o Safari.
- Añada claves de licencia. Consulte Capítulo 4, "Adición de claves de licencia," página 15.
- Si está utilizando la configuración de NAT o de servidor proxy inverso, obtenga la dirección IP o URL accesible externamente que se utiliza en su configuración de implementación. Consulte Capítulo 3, "Configuración de la Aplicación virtual Horizon Mobile Manager," página 13.
- Obtenga la información relacionada con el correo electrónico de su organización para enviar correos electrónicos mediante el servidor de correo SMTP y una dirección electrónica que pueda recibir un correo de configuración de prueba.
- Determine si desea utilizar los valores predeterminados o especifique valores personalizados para los siguientes elementos:

  Base de datos

  Puede utilizar la base de datos vPostgres incrustada (la predeterminada) o su propia base de datos externa. Las siguientes bases de datos externas son compatibles:

  - Microsoft SQL Server 2008
  - Oracle 11g R2

  Por ejemplo, puede que quiera utilizar una base de datos externa en las siguientes situaciones:

  - Para cumplir con las normativas sobre bases de datos de la compañía.
  - Para proporcionar gestión y apoyo mediante las prácticas de gestión de bases de datos estándares de la compañía.
  - Para mejorar el rendimiento o el equilibrador de carga a la hora de gestionar un gran número de usuarios.

	La instalación de Horizon Mobile Manager en una configuración en clúster requiere el uso de una base de datos externa.
Servicio de nombres	Puede utilizar el servicio de nombres OpenLDAP incrustado (el predeterminado) o su propio servicio de nombres. Excepto para las implementaciones de prueba y las iniciales, normalmente utilizará su propio servicio LDAP o Active Directory.
Administrador del sistema predeterminado	Determine qué cuenta de usuario del servicio de nombres seleccionado es la cuenta que desea utilizar como administrador del sistema predeterminado para Horizon Mobile Manager. El administrador del sistema predeterminado puede acceder a la interfaz administrativa de Horizon Mobile Manager y llevar a cabo todas las operaciones. Es una buena práctica limitar el uso de esta cuenta para la configuración inicial de Horizon Mobile Manager, que incluye la asignación de funciones de las operaciones en curso a los usuarios adecuados. Para mantener un seguimiento de auditoría coherente, las operaciones de Horizon Mobile Manager en curso las deben llevar a cabo los usuarios de Horizon Mobile Manager que tienen una función de administrador o administrador del parque asignada. Tras finalizar el procedimiento de configuración e inicialización de los elementos básicos, haga que el administrador del sistema predeterminado inicie sesión en la interfaz administrativa de Horizon Mobile Manager para asignar las funciones adecuadas de Horizon Mobile Manager a los usuarios mediante la página Funciones y trabajos.
Repositorio	Puede utilizar la ubicación predeterminada para el repositorio de Horizon Mobile Manager o especificar otra ubicación. El repositorio almacena objetos de Horizon Mobile Manager como, por ejemplo, imágenes de áreas de trabajo, aplicaciones y archivos de sistema. De forma predeterminada, la ruta del repositorio es `/opt/vmware-mmp/repo` en el sistema de archivos de la aplicación virtual Horizon Mobile Manager. Puede que quiera utilizar un repositorio externo a la aplicación virtual si está utilizando Horizon Mobile Manager en una configuración en clúster o si planea implementar muchas aplicaciones de gran tamaño en áreas de trabajo de los usuarios. Ya que las aplicaciones virtuales tienen un tamaño de disco máximo de 40 GB, si planea implementar muchas aplicaciones de gran tamaño que excedan esa capacidad, seleccione una ubicación de repositorio que tenga una capacidad de almacenamiento adecuada.

NOTA: Puede actualizar los ajustes en la pestaña **Configuración** para una instalación existente de Horizon Mobile Manager en cualquier momento. Sin embargo, la actualización de estos ajustes tras el primer uso de Horizon Mobile Manager puede hacer que sea necesario realizar esfuerzos adicionales para aplicar de forma manual los cambios realizados en el sistema tras el uso inicial. Por ejemplo, si en un principio ha elegido utilizar el servicio de nombres OpenLDAP incrustado y aprovisionar los dispositivos de los usuarios y, a continuación, actualizar la configuración para utilizar un servicio de nombres diferente, los usuarios existentes no funcionarán a menos que se añadan los mismos ID de usuarios al nuevo servicio de nombres.

Procedimiento

1 En su navegador, introduzca la dirección URL de la interfaz de configuración de Horizon Mobile Manager con el formato **`https://`*`dirección_ip`*`:5480`**

2 Inicie sesión como usuario **`root`**.

Utilice la contraseña que estableció cuando configuró la aplicación virtual Horizon Mobile Manager. Si no ha cambiado la contraseña predeterminada, introduzca **`vmware`** como contraseña.

3 Haga clic en la pestaña **Horizon** y haga clic en **Configuración**.

4 En el campo **Nombre del administrador predeterminado**, especifique el nombre de un usuario para que sea el administrador de sistema de Horizon Mobile Manager.

El nombre especificado debe existir en el servicio de nombres que haya seleccionado para Horizon Mobile Manager. El valor predeterminado mostrado (**`admin`**) es una cuenta de usuario en el servicio de nombres OpenLDAP incrustado. Esta cuenta **`admin`** predeterminada tiene la contraseña **`vmware`**.

Si escoge utilizar un servicio de nombres externo, debe actualizar el valor del campo **Nombre del administrador predeterminado** con un nombre que exista en el servicio de nombres.

5 Especifique la ubicación para el repositorio del sistema de archivos de Horizon Mobile Manager.

Es posible introducir una ruta de sistemas de archivos de red o local. De forma predeterminada, la ruta del repositorio es `/opt/vmware-mmp/repo` en el sistema de archivos de la aplicación virtual. Cuando haga clic en **Guardar y reiniciar**, los objetos predeterminados proporcionados por Horizon Mobile Manager (como la imagen base del área de trabajo) se escriben en la ubicación especificada.

6 Escriba una dirección URL raíz (nivel de entrada) accesible externamente para el servidor de inicio de sesión, el servidor de descarga y el servidor de concesiones.

NOTA: Debido a que las áreas de trabajo de los dispositivos móviles gestionados se comunican periódicamente con Horizon Mobile Manager, las URL de los servidores de inicio de sesión, concesiones y descargas deben ser accesibles desde los dispositivos en los que están instaladas o se van a instalar las áreas de trabajo. Si está utilizando la configuración de implementación de servidor proxy inverso o NAT, debe introducir la URL accesible externamente que se utiliza en esa configuración.

Incluya **`https://`** al inicio de las URL. Incluso si ha escrito **`http://`**, el área de trabajo de los dispositivos utiliza el puerto seguro **`443`** para la comunicación con los servidores.

Estas tres URL pueden ser las mismas. Por ejemplo, en una configuración simple de una aplicación virtual Horizon Mobile Manager implementada con una dirección IP pública, esa aplicación virtual puede proporcionar el servidor con fines de administración, inicio de sesión, descarga y concesión. En este escenario, la URL especificada para los servidores de inicio de sesión, descarga y concesión es **`https://`*`dirección_ip`***, donde la *dirección_ip* es la dirección IP pública.

Servidor	Uso
Servidor de inicio de sesión	Lo utiliza el usuario del área de trabajo en el dispositivo móvil para instalar y descargar su área de trabajo.
Servidor de descarga	Proporciona software a las áreas de trabajo.
Servidor de concesiones	Gestiona las concesiones de las áreas de trabajo.

7 (Opcional) Para utilizar su propia base de datos Oracle o SQL Server en vez de la base de datos incrustada, seleccione **Utilizar base de datos externa** y seleccione un tipo de base de datos del menú desplegable. A continuación, especifique la información que permita a Horizon Mobile Manager almacenar y acceder a los datos de la base de datos.

Dirección (URL)	La dirección de la base de datos.
Nombre de usuario	El usuario de la base de datos para la conexión de la base de datos.
Contraseña	La contraseña para la conexión de la base de datos.
Nombre de usuario DBA	Un usuario de la base de datos de nivel DBA con privilegios DDL para crear objetos de base de datos utilizados por Horizon Mobile Manager.

Contraseña DBA	La contraseña para el usuario DBA.
Petición de validación	Petición SQL que se utiliza para validar las conexiones con la base de datos.

Para la base de datos externa, puede especificar ajustes avanzados adicionales, como el tamaño inicial del grupo de conexión.

8 (Opcional) Para utilizar su propio servicio de nombres en vez del servicio OpenLDAP incrustado, seleccione **Utilizar servicio externo** y seleccione el tipo.

Si está utilizando su propio servicio de asignación de nombres de Active Directory, deberá introducir el dominio de Active Directory.

Si está utilizando su propio servicio de asignación de nombres LDAP, deberá introducir la dirección URL del servidor LDAP, el DN de raíz y la consulta de búsqueda de usuario. También es posible introducir el nombre de usuario y la contraseña del DN de gestor.

9 Configure los ajustes de correo electrónico de Horizon Mobile Manager para conectarse con el servidor de correo electrónico de su organización:

a Introduzca la dirección de host SMTP y la información del puerto del servidor de correo electrónico.

b (Opcional) Para utilizar el cifrado SSL, seleccione la casilla de verificación **Utilizar SSL**.

c (Opcional) Para utilizar la autenticación, seleccione la casilla de verificación **Utilizar autenticación** y especifique el nombre de usuario y la contraseña para realizar la autenticación SMTP.

d Pruebe la configuración especificando la dirección de correo electrónico del destinatario y haciendo clic en **Enviar correo electrónico** para enviar un correo electrónico de confirmación.

Si el sistema puede enviar correctamente un correo electrónico utilizando la información SMTP, el correo electrónico de confirmación tendrá un código de verificación.

e Obtenga el código del correo electrónico de confirmación e introduzca el código en el campo **Código del correo electrónico de prueba**.

10 Haga clic en **Guardar y reiniciar** para guardar los ajustes de configuración e inicializar los elementos base necesarios para configurar las áreas de trabajo y gestionar los dispositivos de los empleados mediante Horizon Mobile Manager.

Un mensaje indica que se está llevando a cabo el reinicio.

Cuando se haya finalizado el proceso de reinicio, Horizon Mobile Manager se inicializa y puede iniciar sesión en la interfaz de administración mediante la cuenta del usuario especificada para el administrador del sistema predeterminado.

NOTA: Debe hacer clic en **Guardar y reiniciar** para asegurarse de que los elementos base estén inicializados antes de iniciar sesión en la interfaz de administración. De lo contrario, puede que algunos elementos necesarios no estén disponibles.

Qué hacer a continuación

Ahora podrá configurar los usuarios de áreas de trabajo en Horizon Mobile Manager. En su navegador, introduzca la dirección URL de la interfaz de administrador de Horizon Mobile Manager con el formato **`https://`*`dirección_ip`***

Si especifica el servicio de nombres incrustado y no modifica el valor predeterminado para el nombre del administrador del sistema, puede iniciar sesión en la interfaz del administrador con el nombre de usuario **`admin`** y la contraseña **`vmware`**.

Para obtener más información sobre cómo utilizar Horizon Mobile Manager, tras iniciar sesión consulte la ayuda en línea.

Requisitos de certificado digital de Horizon Mobile Manager

6

Horizon Mobile Manager codifica la información de sesión con certificados digitales estándar. En su configuración predeterminada, Horizon Mobile Manager utiliza certificados generados automáticamente y autofirmados. Utilice el sistema de certificación que mejor se ajuste a su configuración de implementación.

Las comunicaciones entre Horizon Mobile Manager y los dispositivos móviles se envían mediante conexiones con protocolo Secure Sockets Layer (SSL). Horizon Mobile Manager debe presentar certificados válidos a los dispositivos y propagar certificados firmados que se utilizan en las áreas de trabajo en esos dispositivos. Los certificados que se utilizan entre Horizon Mobile Manager y los dispositivos móviles son:

Certificado SSL	Cifra la sesión segura entre el servidor y el cliente (el dispositivo móvil).
Certificado de firma	Firma digitalmente las comunicaciones entre el servidor y el cliente.
Certificados de autoridad de certificación (CA) raíz e intermedia	Proporcione una cadena de confianza de certificado para determinar si se debe confiar en un certificado SSL o de firma concreto.

Cuando instale y configure Horizon Mobile Manager por primera vez, se generará automáticamente un certificado SSL autofirmado y un certificado de firma mediante una autoridad de certificación (CA) raíz interna y la URL especificada para el servidor de concesiones (vea Capítulo 5, "Configuración de los ajustes de Horizon Mobile Manager," página 17). En la página Seguridad de la interfaz de administración de Horizon Mobile Manager aparece una lista de los alias correspondientes a los certificados generados de forma automática.

NOTA: No quite la entrada `internal-ca-root` de la lista **Cadena de certificados de confianza de servidor** de la página Seguridad de Horizon Mobile Manager. Ese certificado es la autoridad de certificación raíz interna que se genera automáticamente y no se debe quitar excepto en condiciones controladas y siguiendo una secuencia de pasos concreta. Para obtener más información, consulte el artículo de la base de datos de conocimientos de VMware en http://kb.vmware.com/kb/2035492.

Aunque estos certificados son únicos y permiten el uso inicial o en prueba de concepto del servidor, no están firmados por una autoridad de certificación conocida y de confianza. Decida si desea sustituir los certificados generados de forma automática por los suyos autofirmados, o por otros firmados por una autoridad de certificación comercial. Para obtener una descripción de la configuración de implementación e informarse de cuándo y cómo utilizar sus propios certificados SSL y de firma, consulte al artículo de la base de datos de conocimientos de VMware en http://kb.vmware.com/kb/2035492.

NOTA: Cuando el certificado SSL es un certificado autofirmado (ya sea el suyo u otro generado de forma automática por Horizon Mobile Manager), antes de iniciar la aplicación VMware® Switch para instalar su área de trabajo corporativa por primera vez, el usuario del dispositivo debe desactivar la casilla de verificación de **Autenticar servidor** en la configuración de la aplicación VMware® Switch. Esa casilla de verificación se selecciona de forma predeterminada. Si la casilla de verificación **Autenticar servidor** no se desactiva y el certificado SSL es un certificado autofirmado, el dispositivo intentará utilizar el almacén de confianza de Android de autoridades de certificación conocidas para verificar el certificado. Como el certificado no está firmado por una autoridad de certificación conocida, la sesión no lo autentica y el dispositivo se niega a conectarse con Horizon Mobile Manager.

Para ver el ajuste **Autenticar servidor** de la aplicación VMware® Switch en el dispositivo, abra la pantalla **Configuración de la aplicación**, toque **VMware Switch** y, a continuación, toque **Administrar espacio**. Si está utilizando un certificado SSL autofirmado, desactive la casilla de verificación **Autenticar servidor**.

Una vez instalada en el dispositivo el área de trabajo corporativa, el usuario puede seleccionar la casilla de verificación **Autenticar servidor** en la configuración de la aplicación VMware® Switch. Tras la instalación inicial del área de trabajo, las comunicaciones emplearán los certificados que contenga dicha área. Si posteriormente el área de trabajo se borra, el usuario deberá desactivar la casilla de verificación **Autenticar servidor** para volver a instalar su área de trabajo, cuando el certificado SSL sea un certificado autofirmado.

Configuración de los ajustes de NDES para usarlos con Horizon Mobile Manager

7

Horizon Mobile Manager incluye un complemento de conector del protocolo de inscripción simple de certificados (SCEP) para el servicio de inscripción de dispositivos de red (NDES) de Microsoft. Este complemento de conector del SCEP admite una conexión entre Horizon Mobile Manager y el servidor NDES de Microsoft de su compañía para automatizar el proceso de creación de certificados digitales para los dispositivos gestionados.

Prerequisitos

- Verifique que está utilizando una versión reciente de los navegadores Chrome, Firefox, Internet Explorer o Safari.
- Añada claves de licencia. Consulte Capítulo 4, "Adición de claves de licencia," página 15.
- Configure los ajustes de Horizon Mobile Manager y haga clic en **Guardar y reiniciar** para inicializar el sistema. Consulte Capítulo 5, "Configuración de los ajustes de Horizon Mobile Manager," página 17.

Procedimiento

1 En su navegador, introduzca la dirección URL de la interfaz de configuración de Horizon Mobile Manager con el formato **`https://`*`dirección_ip`*`:5480`**

2 Inicie sesión como usuario **`root`**.

Utilice la contraseña que estableció cuando configuró la aplicación virtual Horizon Mobile Manager. Si no ha cambiado la contraseña predeterminada, introduzca **`vmware`** como contraseña.

3 Haga clic en la pestaña **Horizon** y haga clic en **SCEP**.

El conector del NDES que proporciona Horizon Mobile Manager está incluido en la lista de conectores SCEP.

4 Haga clic en **Agregar servidor SCEP**.

En la ventana Agregar un servidor SCEP, proporcione la información siguiente:

Nombre del servidor	El nombre del servidor NDES de Microsoft de su compañía.
URL externa	La URL que utilizan los clientes de NDES para comunicarse con el servidor NDES de Microsoft de su compañía.
Conector SCEP	El complemento de conector SCEP utilizado para conectar con el servidor NDES. Se muestra el conector NDES proporcionado.
URL admin	La URL que utilizan los administradores para gestionar el servidor NDES de Microsoft de su compañía.

Nombre de usuario admin	El nombre de usuario del administrador del NDES de Microsoft de su compañía.
Contraseña admin	La contraseña del administrador del NDES de Microsoft de su compañía.
Dominio	El nombre del dominio de Windows en el que se creó la cuenta de administrador del NDES de su compañía.

5 Haga clic en **Agregar** para añadir la información del servidor NDES a Horizon Mobile Manager.

Índice